KEKER & VAN NEST, LLP
JOHN W. KEKER - #49092
MICHAEL H. PAGE - #154913
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

INTERTRUST TECHNOLOGIES CORPORATION
DOUGLAS K. DERWIN - #111407
MARK SCADINA - #173103
JEFF MCDOW - #184727
4800 Patrick Henry Drive
Santa Clara, CA 95054
Telephone: (408) 855-0100
Facsimile: (408) 855-0144

Attorneys for Plaintiff and Counter-Defendant
INTERTRUST TECHNOLOGIES CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant. AND COUNTER ACTION.	Case No. C 01-1640 SBA (MEJ) Consolidated with C 02-0647 SBA **INTERTRUST'S PATENT LOCAL RULE 4-2 PRELIMINARY CLAIM CONSTRUCTIONS AND IDENTIFICATION OF EVIDENCE**

I. Pat.L.R. 4-2(a) Preliminary Claim Constructions

The following constitute InterTrust's proposed definitions for claim terms identified in the parties' Rule 4-1 disclosures. InterTrust reserves the right to modify these definitions in light of definitions, evidence or arguments propounded by Microsoft.

Capitalized terms occurring in definitions represent separately-defined terms and should

be given the same meaning as in the separate definition.

The designation of a definition as "normal English" means that InterTrust believes the defined term should have its normal English meaning, with no definition being necessary. Submission of a definition in such cases does not constitute a waiver of InterTrust's right to contend that no such definition is necessary.

These terms are defined for the claims specified in the definition. InterTrust reserves the right to assert that these terms should be interpreted differently in contexts other than those specified.

Reference citations are to "extrinsic evidence" listed in Section II of this document. Unless otherwise noted, the references constitute dictionaries and the citations are to definitions of the designated terms in such dictionaries.

A. Individual Claim Terms.

Access. (193.15, 193.19, 912.8, 912.35, 861,58, 683.2, 721.34)[1]

To obtain something so it can be used.

References: 1, 2, 6.

Addressing (861.58)

Referring to a location where information is stored.

Reference: 3.

Allowing, allows (912.35, 193.1, 193.11, 193.15, 193.19)

Normal English: permitting, permits; letting happen, lets happen.

Reference: 4.

Applying in combination (683.2)

Using more than one Rule to Govern a Secure Container Governed Item.

Arrangement (721.34)

Normal English: a collection of things that have been arranged. In context, the term can apply to an organization of hardware and/or software and/or data.

Reference: 4.

[1] Patent and Claim numbers are denoted herein in the format "xxx.yy", where "xxx" is the last three digits of the patent number and "YY" is the claim number.

Aspect (900.155, 912.8, 861.58, 683.2)

Feature, element, property or state.

Associated With (912.8, 193.1, 193.11, 193.15, 683.2)

Having a relationship with.

Authentication (193.15)

In context, Identifying (e.g., a person, device, organization, document, file, etc.). Includes uniquely identifying or identifying as a member of a group.

Authorization Information/Authorize/Not Authorize (193.15, 193.19)

Authorize:

Normal English: permit.

References: 4.

Authorization Information:

In context: Information (e.g., a key) received if an action is Authorized. See Specific Information for the definition of Information.

Budget (193.1)

Information specifying a limitation on usage. See Specific Information for the definition of Information.

Reference: 4.

Budget control (193.1)

The term is explicitly defined in the claim as a Control "including a budget specifying the number of copies which can be made of said digital file."

Can be (193.1)

Normal English: the specified act is able or authorized to be carried out. In context, this means the number of copies allowed to be made.

Reference: 4.

Capacity (683.2)

Normal English: "ability," or "capability."

Reference: 4.

Clearinghouse (193.19)

A provider of financial and/or administrative services for a number of users; or an entity responsible for the collection, maintenance, and/or distribution of materials,

information, licenses, etc.

Compares/Comparison (900.155)

Normal English:

Compares: examines for the purpose of noting similarities and differences.

Reference: 4.

Comparison: the act of comparing.

Reference: 4.

Component Assembly (912.8, 912.35)

Components are code and/or data elements that are independently deliverable. A Component Assembly is two or more components associated together. Component Assemblies are executed to perform operating system or applications tasks.

Contained/Contain/Containing (683.2, 912.8, 912.35)

Normal English: to have within or to hold. In the context of an element contained within a data structure (e.g., a secure container), the contained element may be either directly within the container or the container may hold a reference indicating where the element may be found.

Reference: 4.

Control (n) (193.1, 193.11, 193.15, 193.19, 891.1)

Information and/or programming Governing operations on or use of Resources (e.g., content) including (a) permitted, required or prevented operations, (b) the nature or extent of such operations or (c) the consequences of such operations.

Control (v)/Controlling (861.58, 193.1)

Normal English: to exercise authoritative or dominating influence over; direct.

Reference: 4.

Copied file (193.11)

A Digital File that has been Copied.

Copy, copied, copying (193.1, 193.11, 193.15, 193.19)

Reproduce, reproduced, reproducing. The reproduction may incorporate all of the original item, or only some of it, and may involve some changes to the item as long as the essential nature of the content remains unchanged.

References: 1, 4, 6.

Copy control (193.1)

A Control used to determine whether a Digital File may be Copied and the Copied Digital File stored on a second device.

Creating/Creation (861.58)

Normal English: Creating means producing; Creation means the act of creating.

Reference: 4.

Data item (891.1)

A unit of digital information.

References: 2, 3.

Derive/Derives (900.155)

Normal English: obtain, receive or arrive at through a process of reasoning or deduction. In the context of computer operations, the "process of reasoning or deduction" constitutes operations carried out by the computer.

Reference: 4.

Descriptive Data Structure (861.58)

Machine-readable description of the layout and/or contents of a rights management data structure (e.g., a Secure Container).

Designating (721.1)

Normal English: indicating, specifying, pointing out or characterizing.

Reference: 4.

Device Class (721.1)

A group of devices which share at least one attribute.

Digital File (193.1, 193.11, 193.15, 193.19)

A named collection of digital information.

Reference: 3 (definition of "file").

Digitally signing/digital signature (721.1)

Digital signature: A digital value, verifiable with a Key, that can be used to determine the source and/or integrity of a signed item (e.g., a file, program, etc.).

Digitally signing is the process of creating a digital signature.

Entity/Entity's control (891.1)

Entity: A person or organization.

Entity's Control: Control belonging to or coming from an Entity.

Environment (912.35, 900.155, 891.1, 683.2, 721.34)

Capabilities available to a program running on a computer or other device or to the user of a computer or other device. Depending on the context, the environment may be in a single device (e.g., a personal computer) or may be spread among multiple devices (e.g., a network).

References: 6.

Executable Programming/Executable (912.8, 912.35, 721.34)

A computer program that can be run, directly or through interpretation.

Reference: 3.

Execution space (912.8)

Resource which can be used for execution of a program or process.

Execution space identifier (912.8)

Information Identifying an Execution Space. See Specific Information for definition of Information.

Generates/Generating (900.155, 861.58)

Normal English: creates/creating or produces/producing.

Reference: 4.

Govern/Governed/Governed Item (891.1, 683.2)

To Govern: to control an item or operation in accordance with criteria established by the holder of one or more rights relating to the item or operation or a party authorized to establish such criteria.

Governed Item: an item that is Governed.

Reference: 4.

Halting (900.155)

Normal English: suspending.

Reference: 4.

Host Processing Environment (900.155)

This term is explicitly defined in the claim and therefore needs no additional

definition. It consists of those elements listed in the claim.

Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: a Protected Processing Environment incorporating software-based Security.

Identifier (193.15, 912.8)

Information used to Identify something or someone (e.g., a password).

Identify/identifying (193.11, 912.8, 912.35, 861.58)

Normal English: To establish/establishing the identity of or to ascertain/ascertaining the origin, nature, or definitive characteristics of.

Reference: 4.

Including (912.8, 912.35, 900.155, 861.58, 193.1, 193.11, 193.15, 193.19, 891.1, 683.2)

Normal English: depending on the context, this means containing as a secondary or subordinate element, or considering with or placing into a group, class, or total.

Reference: 4.

Information previously stored (900.155)

Normal English: Information stored at an earlier time. See Specific Information for the definition of Information.

Integrity programming (900.155)

This term is fully defined in the claim, which specifies the steps the integrity programming must perform. Integrity programming is programming that performs the recited steps. The term therefore needs no additional definition.

Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: programming that checks the integrity of a Host Processing Environment.

Key (193.19)

Information used to encrypt, decrypt, sign or verify other information.

Load Module (912.8, 721.1)

An Executable unit of code designed to be loaded into memory and executed, plus associated data.

References: 3.

Machine Check Programming (900.155)

Programming that checks a host processing environment and derives information from an Aspect of the host processing environment.

Metadata Information (861.58)

Information about information. Metadata Information may describe the attributes of a rights management data structure as well as processes used to create and/or use it.

Opening secure containers (683.2)

Providing Access to the contents of a Secure Container (e.g., by decrypting the contents, if the contents are encrypted).

Operating environment (891.1)

Environment in which programs function.

References: 6.

Organize, organization, organization information (861.58)

In the context of organization of a Secure Container, these terms refer to contents required or desired (including Information used to categorize these contents); or Information used to specify a particular location for content. See Specific Information for the definition of Information.

Portion (193.1, 193.11, 193.15, 193.19, 912.8, 912.35, 861.58)

Normal English: a part of a whole. The presence of a "portion" does not exclude the presence of the whole (e.g., storage of an entire file necessarily includes storage of any portions into which that file may be subdivided).

Reference: 4.

Prevents (721.34)

Normal English: keeps from happening.

Reference: 4.

Processing Environment (912.35, 900.155, 721.34, 683.2)

Processing: manipulating data.

Reference: 3.

Processing Environment: An Environment used for Processing. A Processing Environment may be made up of one device or of more than one device linked together.

Protected Processing Environment (683.2, 721.34)

~~Processing~~ Environment in which processing and/or data is at least in part protected from Tampering. The level of protection can vary, depending on the threat.

Protecting (683.2)

Normal English: keeping from being damaged, attacked, stolen or injured.

Reference: 4.

Record (912.8, 912.35)

Collection of related items of data treated as a unit.

References: 1.

Rendering (193.11, 193.15, 193,19)

Playing content through an audio output (e.g., speakers) or displaying content on a video output (e.g., a screen).

Required (912.8, 861.58)

Normal English: a thing that is required is a thing that is obligatory or demanded.

Reference: 4.

Resource processed (891.1)

Resource: computer software, computer hardware, data, data structure or information.

Resource processed: a Resource subject to being Processed, i.e., computer software, data, data structure or information. See Processing Environment for a definition of Processed.

Rule (861.58, 683.2)

See Control.

Secure (193.1, 193.11, 193.15, 912.35, 861.58, 891.1, 683.2, 721.34)

One or more mechanisms are employed to prevent, detect or discourage misuse of or interference with information or processes. Such mechanisms may include concealment, Tamper Resistance, Authentication and access control. Concealment means that it is difficult to read information (for example, programs may be encrypted). Tamper Resistance and Authentication are separately defined. Access control means that Access to information or processes is limited on the basis of authorization. Security is not absolute, but is designed to be sufficient for a particular purpose.

Reference: 6.

Secure Container (912.35, 861.58, 683.2)

Container: Digital File Containing linked and/or embedded items.

Reference: 3, 5.

Secure Container: A Container that is Secure.

Secure container governed item (683.2)

Information and/or programming Contained in a Secure Container and Governed by an associated Secure Container Rule.

Secure container rule (683.2)

Rule that at least in part Governs a Secure Container Governed Item.

Secure Database (193.1, 193.11, 193.15)

Database: an organized collection of information.

References: 2.

Database that is Secure.

Secure Execution Space (721.34)

Execution Space that is Secure.

Secure Memory/Memory (193.1, 193.11, 193.15)

Memory: a component of a computer or other device where information can be stored and retrieved.

References: 3, 4.

Secure Memory: Memory in which Information is handled in a Secure manner. See Specific Information for the definition of Information.

Secure Operating Environment (891.1)

An Operating Environment that is Secure.

Securely Applying (891.1)

Requiring that one or more Controls be complied with before content may be used. The operation of requiring that the Control(s) be complied with must be carried out in a Secure manner.

Securely Assembling (912.8, 912.35)

Associating two or more Components together to form a Component Assembly, in a Secure manner. See Component Assembly for the definition of Component.

Securely Processing (891.1)

~~Processing occurring in a Secure manner. See Processing Environment for the definition of Processing.~~

Securely Receiving (891.1)

Receiving has its normal English meaning: acquiring or getting.

Reference: 4.

Securely Receiving means receipt occurring in a Secure manner.

Security (721.1, 721.34)

Relating to being Secure.

Security Level/Level of Security (721.1; 721.34, 912.8)

Information that can be used to determine how Secure something is (e.g., a device, Tamper Resistant Barrier or Execution Space).

Specified information/specific information (912.35, 861.58)

Normal English meaning:

Specific: explicitly set forth or definite.

Reference: 4.

To specify: to state explicitly or in detail.

Reference: 4.

Information: nonaccidental signal(s) or character(s) used in a computer or communication system. Information includes programs and also includes data.

Reference: 4.

Tamper/Tampering (683.2, 721.1, 721.34, 900.155)

To Use (including observe), alter or interfere with in an unauthorized manner.

Reference: 8.

Tamper Resistant/Tamper Resistance (721.1, 721.34, 900.155)

Making Tampering more difficult, and/or allowing detection of Tampering.

Tamper Resistant Barrier (721.34)

Hardware or software that provides Tamper Resistance.

Tamper Resistant Software (900.155)

Software designed to make it more difficult to Tamper with the software.

References: 7, 8.

Use (912.8, 912.35, 861.58, 193.19, 891.1, 683.2, 721.1)

Normal English: to put into service or apply for a purpose, to employ. Reference: 4.

User controls (683.2)

Hardware feature of an apparatus allowing a user to operate the apparatus (e.g., a keyboard).

Validity (912.8)

A property of something (e.g., a Record) indicating that it is appropriate for use.

Virtual Distribution Environment (900.155)

This term is contained in the preamble of the claim and should not be defined, other than as requiring the individual claim elements.

Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: secure, distributed electronic transaction management and rights protection system for controlling the distribution and/or other usage of electronically provided and/or stored information.

Claim Phrases and Clauses

193.1

Receiving a digital file including music (193.1)

See Receiving a digital file (193.11). This phrase is interpreted the same, except that the file includes music.

Budget specifying the number of copies which can be made of said digital file (193.1)

Normal English, incorporating the separately defined terms: a Budget stating the number of Copies that Can Be made of the Digital File referred to earlier in the claim.

Controlling the copies made of said digital file (193.1)

The nature of this operation is further defined in later claim elements. In context, the Copy Control determines the conditions under which a Digital File may be Copied and the Copied File stored on a second device.

Determining whether said digital file may be copied and stored on a second device based on at least said copy control (193.1)

Normal English, incorporating the separately defined terms: Using the Copy Control in deciding whether the Digital File referred to earlier in the claim may be Copied and the Copied Digital File stored on a second device.

If said copy control allows at least a portion of said digital file to be copied and stored on a second device (193.1)

Normal English: a "yes" result is received in the step Determining whether said digital file may be copied and stored on a second device based on at least said copy control (193.1).

Copying at least a portion of said digital file (193.1, 193.11, 193.15, 193.19)

Normal English, incorporating the separately defined terms: Copying at least a Portion of the Digital File referred to earlier in the claim.

Transferring at least a portion of said digital file to a second device (193.1, 193.11, 193.15, 193.19)

Normal English, incorporating the separately defined terms: at least a Portion of the Copied Digital File is sent to a second device.

Storing said digital file (193.1, 193.11, 193.15)

Normal English: that which was transferred in the transferring step is stored.

193.11

Receiving a digital file (193.1, 193.11, 193.15, 193.19)

Normal English, incorporating the separately defined term: a Digital File is obtained.

This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies acts corresponding to this term:

Claim elements specifying the act of receiving a file, or the act of establishing communications, map onto a large number of structures and acts disclosed in the specification, many of which constitute alternate embodiments. These include obtaining a file or communicating through telecommunications links, satellite transmissions, physical exchange of media, network transmissions, etc.

Determining whether said digital file may be copied and stored on a second device based on said first control (193.11)

Normal English, incorporating the separately defined terms: Using the Control to decide whether the Digital File may be Copied and the Copied Digital File stored on the second device.

Identifying said second device (193.11)

Normal English, incorporating the separately defined term: the second device is Identified.

Whether said first control allows transfer of said copied file to said second device (193.11)

Normal English, incorporating the separately defined terms: Using the first Control to decide if the Copied Digital File may be sent to the second device.

Said determination based at least in part on the features present at the device (193.11)

Normal English: the decision referred to earlier in the claim is based at least in part on characteristics of the second device.

If said first control allows at least a portion of said digital file to be copied and stored on a second device (193.11)

See If said copy control allows at least a portion of said digital file to be copied and stored on a second device (193.1). The definitions are the same.

Copying at least a portion of said digital file (193.1, 193.11, 193.15, 193.19)

See Copying at least a portion of said digital file (193.1). The definitions are the same.

Transferring at least a portion of said digital file to a second device (193.1, 193.11, 193.15, 193.19)

See Transferring at least a portion of said digital file to a second device (193.1). The definitions are the same.

Storing said digital file (193.1, 193.11, 193.15)

See Storing said digital file (193.1). The definitions are the same.

193.15

Receiving a digital file (193.1, 193.11, 193.15, 193.19

See Receiving a digital file (193.11). The definitions are the same.

An authentication step comprising (193.15)

Normal English, incorporating the separately defined term: a step involving Authentication.

Accessing at least one identifier associated with a first device or with a user of said first device (193.15)

Normal English, incorporating the separately defined terms: Accessing an Identifier Associated With a device or a user of the device.

Determining whether said identifier is associated with a device and/or user authorized to store said digital file (193.15)

Normal English, incorporating the separately defined terms: deciding whether the Identifier is Associated With a device or user with authority to store the Digital

File.

Storing said digital file in a first secure memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized (193.15)

Normal English, incorporating the separately defined terms: this step proceeds or does not proceed based on the preceding determining step. If this step proceeds, the Digital File is stored in a Secure Memory of the first device.

Storing information associated with said digital file in a secure database stored on said first device, said information including at least one control (193.15)

Normal English, incorporating the separately defined terms: storing a Control Associated With the Digital File in a Secure Database stored at the first device.

Determining whether said digital file may be copied and stored on a second device based on said at least one control (193.15)

See Determining whether said digital file may be copied and stored on a second device based on at least said copy control (193.1). The definitions are the same.

If said at least one control allows at least a portion of said digital file to be copied and stored on a second device (193.15)

See If said first control allows at least a portion of said digital file to be copied and stored on a second device (193.11). The definitions are the same.

Copying at least a portion of said digital file (193.1, 193.11, 193.15, 193.19)

See Copying at least a portion of said digital file (193.1). The definitions are the same.

Transferring at least a portion of said digital file to a second device (193.1, 193.11, 193.15, 193.19)

See Transferring at least a portion of said digital file to a second device (193.1) The definitions are the same.

Storing said digital file (193.1, 193.11, 193.15)

See Storing said digital file (193.1) The definitions are the same.

193.19

Receiving a digital file at a first device (193.19)

See Receiving a digital file (193.11). The definitions are the same.

Establishing communication between said first device and a clearinghouse located at a location remote from said first device (193.19)

Normal English, incorporating the separately defined term: sending information from the first device to the Clearinghouse and/or the first device receiving information from the Clearinghouse.

This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies acts corresponding to this term:

Claim elements specifying the act of receiving a file, or the act of establishing communications, map onto a large number of structures and acts disclosed in the specification, many of which constitute alternate embodiments. These include obtaining a file or communicating through telecommunications links, satellite transmissions, physical exchange of media, network transmissions, etc.

Using said authorization information to gain access to or make at least one use of said first digital file (193.19)

Normal English, incorporating the separately defined terms: the Authorization Information is used in a process of Accessing or Using the Digital File.

Including using said key to decrypt at least a portion of said first digital file (193.19)

Normal English, incorporating the separately defined terms: this step further describes the "using said authorization information" step, and requires that the earlier step include using the Key in a process of decrypting of at least a Portion of the Digital File.

Receiving a first control from said clearinghouse at said first device (193.19)

Normal English, incorporating the separately defined terms: the first device acquires or gets a Control from the Clearinghouse.

This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies acts corresponding to this term:

Claim elements specifying the act of receiving a file, or the act of establishing communications, map onto a large number of structures and acts disclosed in the specification, many of which constitute alternate embodiments. These include obtaining a file or communicating through telecommunications links, satellite transmissions, physical exchange of media, network transmissions, etc.

Storing said first digital file in a memory of said first device (193.19)

Normal English, incorporating the separately defined terms: the Digital File is stored at the first device.

Using said first control to determine whether said first digital file may be copied and stored on a second device (193.19)

See Determining whether said digital file may be copied and stored on a second device based on at least said copy control (193.1). The definitions are the same.

If said first control allows at least a portion of said first digital file to be copied and stored on a second device (193.19)

See If said first control allows at least a portion of said digital file to be copied and stored on a second device (193.11). The definitions are the same.

Copying at least a portion of said first digital file (193.1, 193.11, 193.15, 193.19)

See Copying at least a portion of said digital file (193.1). The definitions are the same.

Transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output (193.19)

See Transferring at least a portion of said digital file to a second device (193.1). The definitions are the same, except that the second device has an audio or video output or both (e.g., a speaker, a screen, etc.).

Storing said first digital file portion (193.19)

Normal English, incorporating the separately defined terms: the Digital File Portion is stored.

721.1

Digitally signing a first load module with a first digital signature designating the first load module for use by a first device class (721.1)

Normal English, incorporating the separately defined terms: generating a Digital Signature for the first Load Module, the Digital Signature Designating that the first Load Module is for use by a first Device Class.

Digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class (721.1)

Normal English, incorporating the separately defined terms: generating a Digital Signature for the second Load Module, the Digital Signature Designating that the second Load Module is for use by a second Device Class. This element further requires that the second Device Class have a different Tamper Resistance or Security Level than the first Device Class.

Distributing the first load module for use by at least one device in the first device class (721.1)

Normal English, incorporating the separately defined terms: distributing the first Load Module so that it can be used by a device in the first Device Class.

Distributing the second load module for use by at least one device in the second device class (721.1)

Normal English, incorporating the separately defined terms: distributing the second Load Module so that it can be used by a device in the second Device

Class.

721.34

Arrangement within the first tamper resistant barrier (721.34)

Normal English, incorporating the separately defined terms: an Arrangement protected by the first Tamper Resistant Barrier, the Arrangement operating as described in the claim.

Prevents the first secure execution space from executing the same executable accessed by a second secure execution space having a second tamper resistant barrier with a second security level different from the first security level (721.34)

Normal English, incorporating the separately defined terms: stops the first Secure Execution Space from executing (e.g. running a program) an Executable accessed by a second Secure Execution space. The first and second Secure Execution Spaces have Tamper Resistant Barriers that have different Security Levels.

683.2

First secure container having been received from a second apparatus (683.2)

Normal English, incorporating the separately defined term: the Secure Container was acquired from a second apparatus. The second apparatus is different from the first apparatus.

Aspect of access to or use of (683.2, 861.58)

Normal English, incorporating the separately defined terms: Aspect and Access to or Use of. Those terms fully define the phrase, so that no other definition is possible.

First secure container rule having been received from a third apparatus different from said second apparatus (683.2)

Normal English, incorporating the separately defined terms: this term requires that the first Secure Container Rule was acquired from a third apparatus. The third apparatus is different from the second apparatus or the first apparatus.

Hardware or software used for receiving and opening secure containers (683.2)

Normal English, incorporating the separately defined terms: computer hardware or programming that acquires Secure Containers and Opens the Secure Containers (see Opening Secure Containers).

This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies structures corresponding to this term:

Structures corresponding to this element include Processor(s) 4126 and/or software running on Processors 4126 (including Protected Processing Environment 650) and Communications Device 666.

Said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers (683.2)

Normal English, incorporating the separately defined terms: the Secure Containers previously referred to are each able to contain a Governed Item, and each Secure Container has an associated Secure Container Rule.

Protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus (683.2)

Normal English, incorporating the separately defined terms: a Protected Processing Environment contains Information. The Protected Processing Environment protects the contained Information from Tampering by a user. The protection may be partial rather than complete. See Specific Information for the definition of Information.

Hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container (683.2)

Normal English, incorporating the separately defined terms: computer hardware or programming that uses the first Secure Container Rule and a second Secure Container Rule. These rules are Applied in Combination to Govern a Governed Item contained in a Secure Container.

This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies structures corresponding to this term:

Structures corresponding to this element include Processor(s) 4126 and/or software running on Processors 4126 (including Protected Processing Environment 650).

Hardware or software used for transmission of secure containers to other apparatuses or for receipt of secure containers from other apparatuses: (683.2)

Normal English, incorporating the separately defined terms: computer hardware or programming that sends Secure Containers to other apparatuses (e.g., other computers) or acquires Secure Containers from other apparatuses.

This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies structures corresponding to this term:

Structures corresponding to this element include Processor(s) 4126 and/or software running on Processors 4126 (including Protected Processing Environment 650) and Communications Device 666.

861.58

Creating a first secure container (861.58)

This term is contained in the preamble of the claim and should not be defined, other than as requiring the individual claim elements.

Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following:

Normal English, incorporating the separately defined terms: Creating a Secure Container.

Including or addressing . . . organization information . . . desired organization . . . and metadata information at least in part specifying at least one step required or desired in creation of said first secure container (861.58)

This is not a claim term, but is instead a series of fragments. Interpretation of this phrase is therefore impossible, since the phrase does not appear in the claim.

At least in part determine specific information required to be included in said first secure container contents (861.58)

Normal English, incorporating the separately defined terms: at least partially Identify Specific Information that must be included in the first Secure Container.

Rule designed to control at least one aspect of access to or use of at least a portion of said first secure container contents (861.58)

Normal English, incorporating the separately defined terms: a Rule that Governs at least some of the contents of the Secure Container.

900.155

First host processing environment comprising (900.155)

A Host Processing Environment including (but not limited to), the listed elements.

Said mass storage storing tamper resistant software (900.155)

Normal English, incorporating the separately defined terms: a mass storage device (e.g., a hard drive) that stores the Tamper Resistant Software.

Designed to be loaded into said main memory and executed by said central processing unit (900.155)

Normal English, incorporating the separately defined term: software designed to be loaded into the Memory of a computer and executed by the computer's processor.

Said tamper resistant software comprising: one or more storage locations storing said information (900.155)

This is not a claim term, but is instead two sentence fragments. Interpretation of this phrase is therefore impossible, since the phrase does not appear in the claim.

Derives information from one or more aspects of said host processing environment (900.155)

Normal English, incorporating the separately defined terms: Derives (including creates) Information based on at least one Aspect of the previously referred to Host Processing Environment. See Specific Information for the definition of Information.

One or more storage locations storing said information (900.155)

Normal English, incorporating the separately defined terms: Information relating to one or more Aspects of the Host Processing Environment is stored in one or more locations. See Specific Information for the definition of Information.

Information previously stored in said one or more storage locations (900.155)

See Information Previously Stored. The definitions are the same.

Generates an indication based on the result of said comparison (900.155)

Normal English: a particular indication is created (e.g., a flag is set or a value is returned) if the comparison has one result, but not if the comparison has a different result.

Programming which takes one or more actions based on the state of said indication (900.155)

Normal English: software that takes an action if the indication has one state, but does not take that action if the indication does not have that state

At least temporarily halting further processing (900.155)

Normal English, incorporating the separately defined terms: Halting Processing, the Halt being temporary or permanent. See Securely Processing for the definition of Processing.

912.8

Identifying at least one aspect of an execution space (912.8)

Normal English, incorporating the separately defined terms: Identifying an Aspect (e.g. Security Level) of an Execution Space

Required for use and/or execution of the load module (912.8)

Normal English, incorporating the separately defined terms: the Identified Aspect is needed in order for the Load Module to execute or otherwise be used.

Said execution space identifier provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security (912.8)

Normal English, incorporating the separately defined terms: the Execution Space Identifier makes it possible to distinguish higher Security Level Execution Spaces

from lower Security level Execution Spaces.

Checking said record for validity prior to performing said executing step (912.8)

Normal English, incorporating the separately defined terms: determining whether the Record has Validity, the determination occurring before the execution step.

912.35

Received in a secure container (912.35)

Normal English, incorporating the separately defined terms: the Record is Contained in a Secure Container when acquired.

Said component assembly allowing access to or use of specified information; (912.35)

Normal English, incorporating the separately defined terms: the Component Assembly allows Access to Specified Information.

Said first component assembly specified by said first record (912.35)

This term is a label referring back to the first component assembly identified earlier in the claim. It has no other meaning.

891.1

Resource processed in a secure operating environment at a first appliance (891.1)

This term is contained in the preamble of the claim and should not be defined, other than as requiring the individual claim elements.

Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following:

Normal English, incorporating the separately defined terms: a Resource Processed in a Secure Operating Environment, the Secure Operating Environment being present at an appliance (e.g., a computer).

Securely receiving a first entity's control at said first appliance (891.1)

Normal English, incorporating the separately defined terms: an Entity's Control is Securely Received at the first appliance.

This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies acts corresponding to this term:

Claim elements specifying the act of receiving a file, or the act of establishing communications, map onto a large number of structures and acts disclosed in the specification, many of which constitute alternate embodiments. These include obtaining a file or communicating through telecommunications links, satellite transmissions, physical exchange of media, network transmissions, etc.

Claim elements specifying the act of "securely receiving" map onto embodiments of "receiving" (see above) in which the received element (e.g., a control) is

received in a manner providing security. The specification describes a number of security-related mechanisms for use in communications, including encryption, authentication and tamper-resistance. Such mechanisms constitute alternate embodiments.

Securely receiving a second entity's control at said first appliance (891.1)

See Securely receiving a first entity's control at said first appliance. The definitions are the same, except that the second entity and the first entity are different.

Securely processing a data item at said first appliance, using at least one resource (891.1)

Normal English, incorporating the separately defined terms: a Resource is used in Securely Processing a Data Item, the processing occurring at the first appliance.

Securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item (891.1)

Normal English, incorporating the separately defined terms: the first Entity's Control and the second Entity's Control are Securely Applied to Govern Use of the Data Item, the act of Securely Applying involving use of the Resource.

II. Designation of Evidence under 4-2(b).

InterTrust hereby designates the following evidence under Patent Local Rule 4-2 (b), without admission that this constitutes "extrinsic evidence" as defined by the Federal Circuit or other relevant legal authority.

Testimony: Dr. Michael Reiter will testify as to the understanding of the claim terms by someone of ordinary skill in the art.

1. Personal Computer Dictionary (1995) ISBN 0-89218-223-7

Access
Copy
Record

2. Computer Professional's Dictionary, Allen Wyatt (Osborne McGraw-Hill, 1990). ISBN 0-07-881705-6

Access
Data Item
Secure database

3. Microsoft Computer Dictionary, Third Edition (1997) ISBN 1-57231-743-4.

Addressing
Copy
Database
Data Item

Environment
Executable File
:
Load module
Memory
Processing
Secure container

4. The American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992) ISBN 0-395-44895-6

Passim

5. U.S. Patent No. 5,634,019, Col 7:42-44.
Secure container

6. Webster's New World Dictionary of Computer Terms, 6th Edition (1997) ISBN 0—02-861890-4

Access
Copy
Environment
Operating environment
Secure

7. U.S. Patent No. 5,991,399.

Tamper resistant software

8. "A Tentative Approach to Constructing Tamper-Resistant Software" by Masahiro MAMBO.\Takanori MU RAYAMAT, Fiji OKAMOTO, School of Information Science, Japan Advanced Institute of Science and Technology,1-1 Asahidai Tatsunokuchi Nomi, Ishikawa/ 923-1211 Japan, published in English 1998.

Tamper
Tamper resistant software

Dated: December 20, 2002

KEKER & VAN NEST, LLP

By: _____
L. JAY KUO
Attorneys for Plaintiff and Counter Defendant
INTERTRUST TECHNOLOGIES CORPORATION

PROOF OF SERVICE

I am employed in the City and County of San Francisco, State of California in the office of a member of the bar of this court at whose direction the following service was made. I am over the age of eighteen years and not a party to the within action. My business address is Keker & Van Nest, LLP, 710 Sansome Street, San Francisco, California 94111.

On December 20, 2002, I served the following document(s):

INTERTRUST'S PATENT LOCAL RULE 4-2 PRELIMINARY CLAIM CONSTRUCTIONS AND IDENTIFICATION OF EVIDENCE

☑ by **PDF TRANSMISSION AND UNITED STATES MAIL**, by transmitting via PDF on this date. A true and correct copy of same was placed in a sealed envelope addressed as shown below. I am readily familiar with the practice of Keker & Van Nest, LLP for collection and processing of correspondence for mailing. According to that practice, items are deposited with the United States Postal Service at San Francisco, California on that same day with postage thereon fully prepaid. I am aware that, on motion of the party served, service is presumed invalid if the postal cancellation date or the postage meter date is more than one day after the date of deposit for mailing stated in this affidavit.

Eric L Wesenberg, Esq.
Mark R. Weinstein, Esq.
Orrick Herrington & Sutcliffe
1000 Marsh Road
Menlo Park, CA 94025
Telephone: 650/614-7400
Facsimile: 650/614-7401

John D. Vandenberg, Esq.
James E. Geringer, Esq.
Kristin L. Cleveland, Esq.
Klarquist Sparkman Campbell, et al.
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland OR 97204
Telephone: 503/226-7391
Facsimile: 503/228-9446

I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

Executed on December 20, 2002, at San Francisco, California.

NOELLE S. NICHOLS